ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC SƯ PHẠM

LƯƠNG THÚY NGA

LÝ THUYẾT VÀNH TRONG MÁY TÍNH

LUẬN VĂN TỐT NGHIỆP THẠC SĨ

Thái Nguyên, năm 2015

ĐẠI HỌC THÁI NGUYÊN
TRƯỜNG ĐẠI HỌC SƯ PHẠM

LƯƠNG THÚY NGA

LÝ THUYẾT VÀNH TRONG MÁY TÍNH

Chuyên ngành: Đại số và Lý thuyết số
Mã số:62.46.01.04

LUẬN VĂN TỐT NGHIỆP THẠC SĨ

Người hướng dẫn khoa học
TS. HOÀNG LÊ TRƯỜNG

Thái Nguyên, năm 2015

LỜI CAM ĐOAN

Tôi xin cam đoan rằng các kết quả nghiên cứu trong luận văn này là trung thực và không trùng lặp với các đề tài khác. Tôi cũng xin cam đoan rằng mọi sự giúp đỡ cho việc thực hiện luận văn này đã được cảm ơn và các thông tin trích dẫn trong luận văn đã được chỉ rõ nguồn gốc.

Thái Nguyên, ngày 10 tháng 4 năm 2015

Người viết luận văn

Lương Thúy Nga

Xác nhận của khoa Toán

Xác nhận

của người hướng dẫn khoa học

TS. Hoàng Lê Trường

LỜI CẢM ƠN

Luận văn này được hoàn thành tại trường Đại học sư phạm - Đại học Thái Nguyên. Trước khi trình bày nội dung chính của luận văn, tôi xin gửi lời cảm ơn chân thành, sâu sắc tới TS. Hoàng Lê Trường (Viện Toán học Việt Nam), thầy là người trực tiếp hướng dẫn, tận tình chỉ bảo, giúp đỡ và động viên tôi trong suốt quá trình nghiên cứu và hoàn thành luận văn.

Tôi cũng xin chân thành cảm ơn ban lãnh đạo phòng sau Đại học, quý thầy cô trong khoa Toán, các bạn học viên lớp cao học Toán k21b đã tạo điều kiện thuận lợi, giúp đỡ, động viên tôi trong suốt quá trình học tập và nghiên cứu tại trường.

Qua đây, tôi xin bày tỏ lòng biết ơn sâu sắc tới người thân trong gia đình, bạn bè đã luôn động viên khích lệ tôi trong suốt quá trình hoàn thành khóa học

Mặc dù có nhiều cố gắng nhưng luận văn vẫn không tránh khỏi những sai sót và hạn chế. Tôi rất mong nhận được những ý kiến đóng góp quý báu của thầy cô và bạn bè để luận văn được hoàn thiện hơn.

Xin trân trọng cảm ơn!

Thái Nguyên, ngày 10 tháng 4 năm 2015

Người viết luận văn

Lương Thúy Nga

Mục lục

MỞ ĐẦU

Mật mã khóa công khai cho phép hai người trao đổi thông tin bí mật, ngay cả khi họ chưa bao giờ gặp nhau và chỉ có thể giao tiếp thông qua một kênh thông tin không an toàn bị theo dõi bởi kẻ thù của họ.

Trong hàng nghìn năm trước đó, tất cả các mã và thuật toán mã hóa đều dựa trên giả định Bob và Alice cố gắng để trao đổi một khóa bí mật mà đối thủ của họ Eve không biết. Bob sử dụng khóa bí mật để mã hóa thông điệp của mình. Alice sẽ sử dụng khóa bí mật tương tự để giải mã thông điệp đó. Eve không biết khóa bí mật nên cô không thực hiện được việc giải mã. Một bất lợi của hệ thống mã hóa bí mật là Bob và Alice cần trao đổi khóa bí mật trước khi họ bắt đầu mã hóa và giải mã thông điệp.

Trong những năm 1970, một ý tưởng đáng kinh ngạc về mật mã khóa công khai bùng nổ. Việc tạo ra các mật mã khóa công khai bởi bởi Diffie và Hellman vào năm 1976 và những phát minh tiếp theo của hệ thống mật mã khóa công khai RSA bởi Rivest, Shamir và Adleman năm 1978 là sự kiện bước ngoặt trong lịch sử của thông tin liên lạc bí mật. Trong một hệ thống mật mã khóa công khai, Alice có hai khóa là khóa công khai K_{pup} và khóa riêng K_{pri}. Alice công khai khóa K_{pup} của cô ấy và Adam, Bob, Carl và mọi người đều có thể sử K_{pup} để mã hóa thông điệp, sau đó gửi thông điệp đã mã hóa cho Alice. Ý tưởng cơ bản của mật mã khóa công khai là mặc dù tất cả mọi người trên thế giới đều biết K_{pup} và có thể sử dụng K_{pup} để mã hóa thông điệp nhưng chỉ Alice biết khóa riêng K_{pri} mới có thể giải mã thông điệp. Bob có thể gửi một thông điệp mã hóa cho Alice ngay cả khi họ không bao giờ được tiếp xúc trực tiếp. Mật mã khóa công khai dựa trên nhiều lĩnh vực của toán học, trong đó đặc biệt là lý thuyết số và đại số trừu tượng (nhóm, vành, trường...).

Mục tiêu của luận văn là bước đầu giới thiệu lý thuyết về mật mã khóa công khai và những ý tưởng toán học cơ bản của lý thuyết đó.

Luận văn được chia làm hai chương. Trong chương một, chúng tôi trình bày một số kiến thức cơ sở về tính chia hết, ước chung lớn nhất, môđun số học, số nguyên tố, phân tích duy nhất, lũy thừa và căn nguyên thủy trong trường hữu hạn, mật mã đối xứng và bất đối xứng... Đây là những công cụ cơ bản dùng cho các định nghĩa và chứng minh ở chương hai.

Chương hai được dành để trình bày về mật mã khóa công khai với các bài toán logarit rời rạc và bài toán trao đổi khóa Deffine-Hellman. Trong phần này chúng tôi còn giới thiệu về hệ thống mật mã khóa công khai ElGamal, thuật toán Pohlig-Hellman và thuật toán gặp gỡ... Phần cuối của chương chúng tôi trình bày lại một số tính chất vành, vành thương, vành đa thức và trường hữu hạn cùng với các bài toán về định lí

thặng dư Trung Hoa.

Vì điều kiện thời gian có hạn nên luận văn vẫn còn nhiều những thiếu sót. Tác giả mong nhận được sự góp ý của thầy cô, các bạn học viên , độc giả quan tâm để luận văn được hoàn thiện hơn.

Thái Nguyên, ngày 10 tháng 4 năm 2015

Người viết luận văn

Lương Thúy Nga

Chương 1

Giới thiệu về mật mã

Nhiều ngành mật mã học hiện đại được xây dựng trên cơ sở nền móng của đại số và lý thuyết số. Vì vậy trước khi tìm hiểu lý thuyết mật mã, chúng ta cần phát triển một số công cụ quan trọng. Trong chương một, chúng ta bắt đầu sự phát triển này bởi việc mô tả và chứng minh các kết quả cơ bản từ đại số và lý thuyết số.

1.1. Tính chia hết và ước chung lớn nhất

Ở mức độ cơ sở nhất, *Lý thuyết số* là việc nghiên cứu về các số tự nhiên

$$1, 2, 3, 4, 5, 6, \cdots,$$

hay tổng quát hơn là nghiên cứu về các số nguyên

$$\cdots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \cdots$$

Tập hợp các số nguyên được ký hiệu là $\mathbb{Z}$. Các số nguyên có thể cộng, trừ và nhân theo cách thông thường, và thỏa mãn tất cả các tính chất thông thường của số học (tính chất giao hoán, tính chất kết hợp, tính chất phân phối,..). Tập hợp các số nguyên với các tính chất của phép cộng và phép nhân là một ví dụ về *vành*.

Nếu a và b là số nguyên, ta có thể cộng $a + b$, trừ $a - b$ và nhân $a \cdot b$. Trong mỗi trường hợp, chúng ta được kết quả là một số nguyên.

Tuy nhiên, nếu chúng ta muốn kết quả là số nguyên, chúng ta không thể luôn luôn chia một số nguyên bởi số nguyên khác. Ví dụ, chúng ta không thể chia 3 bởi 2, vì không có số nguyên bằng $\frac{3}{2}$. Từ đó dẫn đến các khái niệm cơ bản của tính chia hết.

Định nghĩa 1.1.1. Cho a và b là số nguyên với $b \neq 0$. Ta nói rằng b chia hết a, hay a được chia hết bởi b, nếu có một số nguyên c sao cho

$$a = bc.$$

Ta viết $b \mid a$ thay cho b chia hết a. Nếu b không chia hết a, thì ta viết $b \nmid a$.

Ví dụ 1.1.2. Ta có $5 \mid 20$, vì $20 = 5 \cdot 4$, $6 \nmid 20$, vì $20 = 6 \cdot 3 + 2$, vì vậy 20 không phải là bội của 6.

Nhận xét 1.1.3. Mỗi số nguyên đều được chia hết bởi 1. Những số nguyên được chia hết bởi 2 được gọi là số chẵn, và những số nguyên không được chia hết bởi 2 được gọi là số lẻ.

Mệnh đề 1.1.4. Cho a, b, c là số nguyên. Khi đó, các mệnh đề sau là đúng.

1. Nếu $a \mid b$ và $b \mid c$, thì $a \mid c$.
2. Nếu $a \mid b$ và $b \mid a$, thì $a = \pm b$.
3. Nếu $a \mid b$, và $a \mid c$, thì $a \mid (b + c)$ và $a \mid (b - c)$.

Chứng minh.

1. Vì $a \mid b$ và $b \mid c$ nên tồn tại $a_1 \in \mathbb{Z}$ và $b_1 \in \mathbb{Z}$ sao cho $b = aa_1$ và $c = bb_1$. Ta có $c = (aa_1)b_1 = a(a_1b_1)$, do đó $a \mid c$.
2. Vì $a \mid b$ và $b \mid a$ nên tồn tại $a_1, b_1 \in \mathbb{Z}$ sao cho $b = aa_1$ và $a = bb_1$. Ta có $b = (bb_1)a_1 = b(b_1a_1)$. Do đó $a_1b_1 = 1$ và $a_1 = b_1 = \pm 1$. Vậy $a = \pm b$.
3. Vì $a \mid b$ và $b \mid c$ nên tồn tại $a_1, a_2 \in \mathbb{Z}$ sao cho $b = aa_1$ và $c = aa_2$. Do đó $b + c = a(a_1 + a_2)$ và $b - c = a(a_1 - a_2)$. Vậy $a \mid (b + c)$ và $a \mid (b - c)$.

□

Định nghĩa 1.1.5. Ước chung của hai số nguyên a và b là số nguyên dương d chia hết cả a và b. Ước chung lớn nhất của a và b là số nguyên dương lớn nhất d sao cho $d \mid a$ và $d \mid b$. Ước chung lớn nhất của a và b được kí hiệu là $\gcd(a, b)$ hay (a, b). (Nếu a và b bằng 0, thì $\gcd(a, b)$ không xác định.)

Ví dụ 1.1.6. Ước chung lớn nhất của 12 và 18 là 6.Tương tự ta có, ước chung lớn nhất của 748 và 2024 là 24. Một cách kiểm tra là liệt kê tất cả các ước nguyên dương của 748 và 2024.

$$\text{Ước của } 748 = \{1, 2, 4, 11, 17, 22, 34, 44, 68, 187, 374, 748\}.$$
$$\text{Ước của } 2024 = \{1, 2, 4, 8, 11, 22, 23, 44, 46, 88, 92, 184, 253, 506, 1012, 2024\}.$$

Kiểm tra hai dãy trên, ta thấy ước chung lớn nhất của 748 và 2024 là 44. Từ ví dụ này ta thấy, đây không phải là phương pháp hiệu quả. Nếu cần tính ước chung lớn nhất của các số lớn, ta sẽ phải tìm phương pháp khác hiệu quả hơn.

Chìa khóa để tìm thuật toán hiệu quả hơn cho việc tính ước chung lớn nhất là phép chia có dư. Do đó nếu a và b là số nguyên dương và nếu chia a bởi b, chúng ta sẽ được thương q và số dư r, phần dư r nhỏ hơn b. Ví dụ 230 được chia bởi 17, ta được thương là 13 với số dư là 9, tức là $230 = 17 \cdot 13 + 9$, với số dư 9 nhỏ thực sự hơn số chia 17.